Global Information Assurance Certification Paper

Identity Theft:
What you need to know

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1 - Research on Topics
In Information Security

Submitted by: Krzysztof Biernacki

September 21, 2004

Abstract

We all know that we are unique, but most of us don't realize that protecting our personal identity is a constant battle. A serious problem that is on the rise in Canada as well as in other countries is identity theft. Identity theft can be defined as “when an unscrupulous person gathers enough information about you to successfully impersonate you online, by mail, over the telephone, or in person.”[1]

This paper will discuss the importance of 3 types of personal identification, techniques used by criminals to gather your personal identification, steps you can take to protect yourself against this type of crime, and what to do if you become a victim of identity theft.

Introduction

We all work hard to create our own identity, be it either by having a crazy hairdo, or owning a flashier car or bigger house than our neighbours. But when it comes to safeguarding our own personal information, the information that makes us who we are, we all fail miserably. The theft of one’s personal information, referred to by many as identity theft, continues to rise. According to the Better Business Bureau of Canada, “Identity theft costs Canadian Consumers an estimated 2.5 billion annually and an overall cost of 5 billion to the Canadian Economy."[2] The Federal Trade Commission stated that, “More than 9.9 million Americans were struck by identity thieves in 2003, costing individuals and businesses $52.6 billion in expenses.”[3] Unfortunately this problem will continue to become worse rather than better, due to advancements in technology such as computers, photo copiers, camera phones, scanners, and the aid of digitized online information.

Identity theft is any form of criminal activity that involves the act of assuming the role of another individual, through the use of their personal information such as Birth Certificate, Social Insurance Number, or Driver’s License. Criminals can use this information to do a variety of things including opening new credit card accounts, obtaining loans, renting apartments, or even obtaining a passport. Unfortunately many of us don’t realize how easy it is for anyone, not just criminals or cyber criminals, to obtain our personal information. Robbing someone on the street or entering their home unlawfully is no longer needed. Methods of obtaining your personal information are becoming even more sophisticated and cunning.

---

[1] “Glossary-Access eGovernment”, Internet, http://www.access-egov.info/glossary.cfm?xid=NE
[2] “Identity Theft - Robbery in the New Millennium”, Internet, http://www.cbc.ca/consumers/indepth/identity/index.html
[3] “What's your online broker doing to prevent ID theft?”, Internet, http://www.globalsecurity.org/org/news/2003/031121-id-theft01.htm

In this essay I will discuss 3 critical pieces of personal identification and their value, techniques criminals use to compromise your identity, additional ways to protect yourself, and steps to take if you become a victim of identity theft.

3 Critical pieces of Personal Identification

Understanding the value of your personal information is crucial in your fight against identity theft. We are very careless when it comes to protecting the information that makes us who we are. The reason for this is our lack of knowledge or understanding of why anyone would want our Social Insurance Number (SIN), Driver's License or even our Birth Certificate.

Recently a colleague of mine conducted a survey at his place of employment to find out how many of his fellow employees had their SIN in their possession at all times and the reason they carried it with them. He conducted this survey allowing the employees that participated to remain anonymous, the group that took part involved 20 people, 9 men and 11 men, ages varying from 23 – 53 years of age.

The results were a little disturbing. In response to the question of where their SIN was, 60% percent of them responded that they carried it with them in their wallets or purses at all times, 30% responded that it was somewhere at home in a desk drawer or in a box somewhere, and 10% responded that they had lost it at some point and did not know where it was. When asked why they did or did not carry it, 20% responded that they didn't carry it with them because they didn't need it because they knew the SIN by heart. The other 80% responded by either stating; "why not carry it?" or a simple, "I don't know why I carry it."

The majority of us don't understand the value of certain personal information before it's too late.

Many people assume that identity theft won't happen to them, because they don't shop online. They think their information isn't stored anywhere so it can't be compromised. What these people don't realize is identity theft occurs everywhere, not just online. So how can my Personal Information such as my SIN, Driver's License, and my Birth Certificate have any value to someone else? These 3 pieces of identification all serve different purposes, and are obtained in different ways. There are certain people who you should and shouldn't give this information to, and the consequences of this information falling into the wrong hands are different.

Social Insurance Number

What is it and what is it used for?

This nine digit number that is referred to as your SIN is required for an individual to secure legal employment in Canada or receive any form of Government benefits. It was to be used in conjunction with the administration of various other

Canadian Government programs, such as the Canada Pension Plan and Employment Insurance.

Some organizations, however, use the SIN for their numbering system. The SIN has become an identifier or account number for these organizations so that they don't have to set up or create their own numbering system. Quite a few dental plans out there use your SIN as an identifier. Organizations are not breaking the law by doing this, as there is no legislation that prohibits companies or groups from asking you for it. One of the most ignored facts about the SIN is that it has become the primary piece of information that is required when you apply for a credit card or open a bank account.

Obtaining a SIN isn't complicated at all. You can either visit your nearest Human Resources Development Canada office or you could even apply for a SIN by mail, complete an application form, with the supporting identity document(s), and fee. Currently when applying for a SIN the only primary document you require is a Birth Certificate issued in Canada by the vital statistics branch of your province or territory of birth. You are not required to provide any form of picture identification.

Who should and shouldn't have or know your Social Insurance Number?

You should always be aware of who requires what type of information from you. There are a few legitimate situations where you will need to provide your SIN, for example, to your employer. An employer can collect an employee's SIN to provide you with Records of Employment and T-4 slips for income tax purposes, as can provincial or municipal agencies to report financial assistance payments for income tax purposes. Financial Institutions from which you earn interest or income, such as banks, credit unions and trust companies, must also ask for your SIN.

When an individual or organization asks you for your SIN, always ask why they require it, how will it be used, where will it be stored and to whom it will be given. If it's not required by law, or you are not satisfied with the explanation they offer you in return, tell them that you would prefer not to use that particular type of identification and offer an other form of identification. If you are refused service or products unless you provide them your SIN, complain to the Privacy Commissioner of Canada. Remember - your SIN should never be used as a piece of identification.

To view other Legislative uses of the SIN please see:
(http://www.privcom.gc.ca/fs-fi/02_05_d_02_e.asp)

What havoc could a criminal potentially do with your Social Insurance Number?

The reality is what *can't* they do with the knowledge of your SIN and the information it can provide for them. For example, a criminal or identity thief could be standing right behind you in line when you are paying for groceries at the grocery store. You decide to use your credit card which you carry along with other pieces of identification in your wallet or purse. What you don't notice is the person behind you in line, having a so-called conversation on their cell phone (not a regular cell phone but a new camera cell phone). You may think nothing of it, but just when you are removing your credit card from your wallet or purse that person took a quick picture of the front of the card. They now have the 16 digit card number and the type of credit card it is. They waited for you to sign the receipt and took another picture so they now have your signature. When you were putting your credit card away they took another snapshot of your wallet or purse to have a picture of all it's contents. They do this because chances are you are carrying your SIN along with your other types of identification.

When they go home they download their new pictures of your items onto their PC. Even if the pictures are blurry there are many types of software that will improve the clarity of the pictures. They can now read the numbers of your SIN, your address and birth date on such types of identification as your Driver's License.

They can begin by calling your credit card company and answer a few basic security questions which they already know the answers to: such as birth date, and SIN. They confirm with the credit card company your credit limit and can then begin purchasing goods without ever raising an alarm. In most cases they wouldn't have been able to get this far if they had not known your SIN or if you had not given them that opportunity to take those pictures.

How do you protect your Social Insurance Number?

You should never be carrying it in your wallet or purse unless its absolutely necessary, have it memorized instead. If you are asked to provide it over the phone, verify the person or organization by calling them back, or state to them that you would rather provide this information in person. When providing this information be aware of who is listening around you or where your SIN is being written or devices it is being stored in.

This personal type of information as well as others of it's kind should be stored in a secure place such as a safety deposit box. Carrying your SIN makes you that much more susceptible to identity theft. Think of the amount of valuable information a criminal would have if they had your SIN card, Driver's License and your Birth Certificate if you were to carry them all at once in your wallet or purse.

Men are just as bad as women when it comes to carrying too many credit cards and personal identifiers in their wallets as women are in their purses.

Driver's License

What is it and what is it used for?

The sole purpose of a Driver's License was to prove that you are authorized by law to operate a vehicle. By law you must possess this identification on you when you are in operation of a moving vehicle. Disappointingly though, it has become the most commonly acknowledged and trusted picture identification card issued by the government. When you are purchasing lottery tickets, alcohol or renting a video, this is the primary identification that most businesses will require or ask of you to prove that you are of age or to confirm that you are who you say you are.

How do you get one?

Once you have reached the minimum age requirement which is usually age 16, you can begin the process of getting a Driver's License. To obtain a valid Driver's License you begin by applying in person to write a knowledge test for a Learner's Permit. You will be asked to provide a primary piece of identification, usually a Birth Certificate, as well as a secondary piece of identification, usually a SIN, along with a fee. Eventually after a probationary period, you are allowed to take a road test at a Driver's Service Centre.

Who should and shouldn't have your Driver's License?

Since the Driver's License has become such a widely recognized identity card, not using it is nearly impossible. By law, law enforcement agencies require you to provide it to them when you are in operation of a moving vehicle.

What havoc could a criminal potentially do with your Driver's License Number?

If your Driver's License is lost or stolen the damage can be devastating and the cleanup afterward will be endless. If it were tampered with to display your information or information of someone else's choice such as another picture or age, it could be used for someone else's financial gain. By itself, or in conjunction with other forms of identification, a Driver's License can be used to create bank accounts, apply for credit cards, or compile traffic fines. These are just a few ways criminals can begin destroying your good credit rating, driver's record or identity. Financial crime is nothing compared to what other criminals such as terrorists could potentially do. The September 11 attackers apparently had legal documents obtained either through alternate sources such as altered Driver's Licenses, Birth Certificates as well as SINs.[4]

[4] "Identity Theft - Robbery in the New Millennium", Internet, http://www.cbc.ca/consumers/indepth/identity/

How do you protect your Driver's License?

You begin by changing the default password on your Driver's License account at your local Driver's Service Centre. They will either charge you a fee or you can wait until it is time to renew it. When people first obtain their Driver's License, most keep the default password on their account (in most cases their mother's maiden name). Since this is one type of identification you usually require to have in your possession, do not leave out in the open or store it in a non-secure location such as your vehicle's glove compartment. If someone asks to see your Driver's License always ask them why and what will it be used for. It is your right to question any request someone may have of you when conducting any type of business. When you are providing it to tellers or clerks to confirm your identity when using a credit card or making a purchase with a check, be sure that it never leaves your sight or is photocopied. When they ask you for your Driver's License Number when you are applying for a loan or credit card, always ask them why and where it will be stored. If you are asked to provide it over the phone, as with your SIN, verify the person or organization by calling them back or state to them that you would rather provide this information in person. When providing this information be aware of who is listening around you and where your Driver's License number is being written or devices it is being stored in.

Birth Certificate

What is it and what is it used for?

A Birth Certificate is issued to you when your birth is registered with the Vital Statistics Agency. Unless your birth is registered, you will not be issued a legal Birth Certificate. To order a Birth Certificate you may either apply in person at your local Vital Statistics Office or Government Agent office, or you may apply by mailing an application for service form with the appropriate fee. The Birth Certificate is unique because it does not have an expiry date. The government requires the proof of a Birth Certificate when applying for any provincial or federal program such as a SIN or a passport.

Who should and shouldn't have your Birth Certificate?

When we were young, we didn't know what a Birth Certificate really was or the importance of one. Most of our guardians stored them for us in a secure location so we didn't lose them, and gave them to us only when we showed some sense of responsibility. More than likely, most of us don't even know where our Birth Certificates are!

Today, it is very important to know where it is at all times. Your Birth Certificate is a vital piece of your personal information; most of us didn't need to personally use it until we were applying for our Driver's License, Passport or for proof of Canadian Citizenship when applying for college or university. With today's

immense concerns regarding terrorism, your Birth Certificate is the last piece of identification you'd want to fall into the wrong hands.

What could a criminal potentially do with your Birth Certificate?

The Birth Certificate is the one document that can be used to gain access to all of your other information. It can also be used to obtain or apply for other government issued identification such as Driver's License, passports and your SIN.

A criminal can begin by reapplying for your SIN by walking over to the nearest Human Resources Development Canada (HRDC) Office or they could even apply for a SIN by mail. They complete an application form, and they state that they are you and require a new SIN card as they have lost their previous one. They provide your Birth Certificate which they have in their possession as it was in the wallet they had stolen from you or you had lost. As they apply for the new card, they decide to change your current mailing address that HRDC has on file. The identity thief changes it to an address that is more convenient to them. Now the new SIN card is mailed to them within three weeks of submitting the application at which point your nightmare begins without you even being aware of it.

Since they have your Birth Certificate and your SIN, they can begin applying for credit cards, opening bank accounts, creating cell phone accounts, and even rent apartments. They can walk away from all bills and damages, which are now your responsibility to pay. The onus is on you to begin the long road of cleaning up the damage they have done with your creditors.

How do you protect your Birth Certificate?

Your Birth Certificate should be stored in a secure place such as a safety deposit box. You should only have it in your possession the day you will need it. If you are required to have certain documents when traveling, make photocopies of the originals so that you can provide authorities with the information that they require if you need to reapply for replacements. Carrying your Birth Certificate makes you that much more susceptible to identity theft, especially if you are in the habit of carrying all your identification with you at once.

Techniques Used by Identity Thieves.

There are several other techniques used by criminals to commit identity theft. These are just a few.

Dumpster Diving

What is it?

It is exactly what it sounds like: rummaging through one's trash. Why would someone want to go through another person's trash? For one important reason: people throw away valuable information. Criminals are hoping that they will discover a credit card statement, telephone bill, Income Tax statement anything that someone didn't tear up. These can be used to discover other types of valuable information about a person. We think its garbage, but to the right person it is like finding treasure at the bottom of the ocean.

What are the consequences?

We all receive those annoying letters that contain "pre-approved credit-card offers". How many of us actually go out of our way and destroy them by shredding them or ripping them to pieces? These letters can be sent by a criminal to the issuing financial institution requesting that the card be sent to the recipient, but at a new address that is more convenient for the identity thief. Many of us throw away insurance forms, cheques, financial statements, old income tax returns, etc... rather blindly. Remember, bills can contain information such as your full legal name, your mailing address, and how many people live in your household. Your credit card statements will reveal what you owe and your available credit limits. What identity thief wouldn't want that kind of information? They will now know how much they can spend without someone being alarmed. They will also know your billing cycle so they will know how much time they have to use it without arising suspicion from you.

Inadvertently you are helping the identity thief commit fraudulent purchases. Even worse though someone could determine where you were born and apply for a Birth Certificate.

What can be done to prevent this?

This can all be avoided by purchasing a $20 paper shredder at Wal-Mart. You should be shredding or destroying sensitive documents that may contain information about you before disposing of them.

Mail Redirection Fraud

What is it?

Mail redirection is when an individual, family or business has their mail rerouted to an alternate address rather than the current one. Mail can be redirected to Canada, the U.S.A. or to international destinations. Mail redirection fraud occurs when an unauthorized party redirects your mail to an address of their choice.

What are the consequences?

In 2001, Canada Post caught 400 cases of fake address changes, a 10 fold increase from the year before. Since then, thousands of cases have been reported.[5] Canada Post requires someone to visit a Canada Post Outlet and fill out a change of address form. They require two pieces of identification, one with a photo and one with your current address and signature. Change of address requests can also be done online. All that you are required to have is a current and forwarding address, valid credit card (VISA, MasterCard or American Express), valid e-mail address and a web browser that supports 128-bit encryption.[6]

We already have determined how easy it would be to obtain those pieces of identification. Canada Post charges $33 for six months to redirect your mail. This is all that is required to have all the mail going to your household to be redirected. Think of how easy it would be for a criminal to have your mail redirected to a Post Office box located somewhere convenient to them. All your future statements from your Bank, Phone Company, etc… that contain so much valuable data are now in the hands of the crook. When your mail is redirected, it will take even more time for you to realize what has happened and give more time to the identity thief to commit further frauds.

What can be done to prevent this?

Be aware of bills and statements that don't arrive when they are supposed to, this will be a clear indication that either mail has been stolen or your mail has been redirected to alternate address. If possible you should be locking your mailbox. If you are going away arrange for a trustworthy relative or friend to pick up your mail or you can even ask for Canada Post to issue a Hold Mail service. A Hold Mail service is when all your mail is held by Canada Post for specified period of time. There is a charge for this service.

You should also think twice about displaying your family name anywhere on the outside of your mailbox or on the front of your home. Identity thieves would only need to look up your last name in the phone book to determine your first name. They could then redirect your mail and commit any other fraud they may want. Remember, the least amount of information someone may have about you the better. Some people may think it's weird or impolite to withhold information, but at least you are being proactive in your attempts to safeguard your privacy.

[5] "Identity Theft - Robbery in the New Millennium", Internet, http://www.cbc.ca/consumers/indepth/identity/index.html
[6] "Mail Redirection", Internet, http://www.canadapost.ca/common/offerings/supplementary_services_pers/can/redirection_permanent-e.asp

Card Skimming

What is it?

Remember those of us who said that we were safe from identity theft because we don't shop online? Well what about when we dine out at a restaurant or pay for gas with our credit cards? Identity thieves don't necessarily look how we expect them to. They could be that nice waitress or gas attendant that you just handed your credit card to. They may swipe your card through an electronic device known as a Skimmer.

A Skimmer is a device usually the size of credit card. It can fit in your back pocket or in the palm of your hand. It records the data from the magnetic strips on the back of the cards.

What are the consequences?

The credit card information they get from swiping your card is stored in the Skimmer and then sold or communicated to another location, sometimes overseas. It is then re-encoded onto illegally made credit cards. Criminals can then either sell or use these fraudulent credit cards. Unfortunately, because it is your information on the card, you are responsible for paying for the charges and cleaning up the mess with your creditors.

What can be done to prevent this?

You should always have your card in plain eyesight. Be sure to monitor your monthly statements and immediately report any unauthorized activity. Most creditors will usually question any large purchases made on a credit card by calling you to confirm you did make that purchase. You can have this amount modified to a smaller amount so the likelihood of discovering unauthorized purchases increases. To avoid this completely pay with cash, it still exists.

Phishing

What is it?

Another scam that is gaining ground on the Internet today is phishing. This is a new technique of online identity theft that is being used mainly by organized crime, in the former Soviet, and Asia. However, it is becoming more prevalent in North America.[7]

Unlike spam, which attempts to ploy the recipient to purchase porn or male enhancement drugs, criminals attempt to fool the unsuspecting user with the

[7] "Hooked." Information Security. July 2004, http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss426_art874,00.html?track=NL-358&ad=487004

fabrication of emails that contain links to websites or forms. To the untrained individual these appear to be from legitimate companies, such as financial institutions (Citibank)[8] or online sites (eBay).[9] These emails are aimed to have customers of these sites enter or reply to the email with a large amount of personal information such as credit card numbers, usernames and passwords.

What are the consequences?

What happens eventually with this information is that it is sent to a redirected location that the criminal created. Using this personal data they can begin to commit several fraudulent schemes such as online purchases with your credit card, in some cases through the same website they are imitating. The recent Gartner study estimates that 30 million Americans have received a phishing attack, and about 3 percent (1.78 million) submitted personal and/or financial information.[10] Some sources believe the response rate to be as high as 5 percent.[11]

What can be done to prevent this?

It is very important that you are aware that such frauds are circulating on the Internet. Always remember that no company will ever send you an email to verify your username or password, or ask you for any financial information. If you have any doubts contact the company directly via their customer service phone number or customer service email which will be located directly on most companie's websites.

Additional Steps to Protect Yourself

Identity theft is not going to slow down anytime soon, as Criminals do not seem to be too concerned with strict fines and long prison terms. In Canada, identity theft does not even have a statutory definition, although under the criminal code, impersonation with intent will net someone a prison term of up to 10 years. The presiding judge could also decide if the identity thief should receive any fines or pay any sort of restitution to their victims. The only charge that could be laid upon someone would be fraud, which itself could only lead to a 10 year prison term. However, fines for providing false information when applying for vital documents such as Birth Certificates have increased from $1,000 to $50,000 and/or jail sentences of up to 2 years for individuals and up to $250,000 for

[8] "Hooked." Information Security. July 2004, http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss426_art874,00.html?track=NL-358&ad=487004
[9] "Hooked." Information Security. July 2004, http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss426_art874,00.html?track=NL-358&ad=487004
[10] "Hooked." Information Security. July 2004, http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss426_art874,00.html?track=NL-358&ad=487004
[11] "Hooked." Information Security. July 2004, http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss426_art874,00.html?track=NL-358&ad=487004

corporations[12].But there are still too many gaps in the criminal law that need to be addressed; it needs to be restructured to designate certain forms of fraudulent activities as crimes.

Recently in the United States, President Bush signed the Identity Theft Penalty Enhancement Act, which increases the minimum amount of prison time for those convicted of using someone else's identity to commit fraud, terrorism, and other crimes. During the signing ceremony, Bush stated the law, "sends a clear message that a person who violates another's financial privacy will be punished."[13]

Hopefully the Canadian government will soon follow suit and increase penalties and fines towards individuals caught in any form of Identity Theft.

Individual agencies have also begun or are considering taking steps to improve themselves. The Human Resources Development Canada (HRDC) is currently reviewing the entire process surrounding the SIN and is looking for better ways to improve the security and integrity of the system.[14] Driver's License issuing centers are working to make it more difficult to counterfeit Driver's Licenses and to strengthen the policies used when issuing licenses.[15] Some experts believe that Birth Certificates will cease to exist within five years, as plans for an electronic births, deaths and marriages registration system are rolled out. Apparently the general public will not require a paper Birth Certificate as government agencies will be able to check the National Database electronically.[16]

We cannot just hope that law enforcement agencies or governments protect us against these criminals. We as individuals have a role to take in preventing identity theft. We must be alert to the risk and threat of identity theft, and protect our personal information. Some other helpful guidelines are:

- Know your billing cycle from your phone company to your creditors. Be sure to follow up with them immediately if the delivery of bills isn't on time, or if there are any discrepancies in your monthly statements. Sometimes mail could have been delivered to the wrong house or just lost or an honest error been made. These things happen, but you must always follow up with them so that they are aware and can put an alert on your account and investigate.

[12] "Identity Theft - Robbery in the New Millennium", Internet, http://www.cbc.ca/consumers/indepth/identity/
[13] "President Signs Identity-Theft Law", Internet, http://informationweek.com/story/showArticle.jhtml?articleID=23901861
[14] "Changes to protect the integrity of the Social Insurance Number ", Internet, http://www.hrsdc.gc.ca/en/cs/comm/news/2002/021008_e.shtml
[15] "National Poll Indicates Americans Favor Congressional Action to Strengthen Driver's License/ID Security" Internet, http://www.aamva.org/news/nwsPressReleaseNationalPollIndicatesAmericansFavorStrongerID.asp
[16] "IT ends paper births register", Internet, http://www.vnunet.com/print/1157422

- When using an ATM machine you should be using your hands or body to conceal the keypad and screen. When using your credit card to purchase goods or services, hand it to the teller or clerk face down, and conceal the signature with your thumb or palm. Always remember if someone is giving you a bad feeling or standing a little to close to you, it is in your best interest either to wait until they have left before completing your transaction or ask them kindly to provide you with more space.

- Do not reveal any type of personal information, such as your birth date, your mailing address, your SIN, your full legal name unless you are aware of how it will be used, if it will be shared and how will it be stored or destroyed when they are through with it. Live by the policy on a "need to know basis". Be Defensive, never reveal this information over the phone or through the Internet unless you have initiated contact.

- Routinely destroy all credit cards once expired or any cards that you no longer use. Keep a list of the ones that you use regularly. You should also get into the habit of signing the back of credit cards or debit cards and to write a small note underneath your signature to ask for picture identification. The merchant then knows to ask for this. If they don't (which happens often) you may want to bring this to a manager's attention or consider shopping elsewhere.

- Almost all companies will give you an option to have passwords placed on your accounts. If you place a unique password on your account this will make it more difficult for someone pretending to be you, to access your personal information. Try to avoid using the default recommendation which is usually your mother's maiden name, and try to have different passwords for each account. If they ask for you to use your SIN as an identifier ask to use something else. Always try to avoid keeping a written record of your account passwords as well as your computer passwords. If you must write them down and can't memorize them all, make sure they are well disguised by rearranging the numbers with letters or symbols and storing that list in a secure location.

- When paying for gas at the pump, or withdrawing money out of a bank machine. Under no circumstances leave receipts behind, make certain you destroy them and any other paperwork you no longer need. Remember those receipts contain your full credit card number, expiration date, as well as display if it were a MasterCard, Visa Card, or American Express.

- Obtain a copy of your credit report once or twice a year from either Equifax or TransUnion, to ensure that there hasn't been any sort of activities that you have not approved.

These are just a few of the steps that you should be doing on a daily basis to ensure that your personal information does not fall in the wrong hands and you become a victim of identity theft. Sadly, the damage that identity theft can cause and the long road in repairing that damage is frustrating. Chances are if you aren't already taking preventative steps to guard against it you are probably a victim already. Don't try telling yourself that you don't have the time to take precautions, because if you have time to surf the Internet or respond to an email you have time to protect yourself.

What do you do if you are a victim of Identity Theft?

The first thing you need to do is contact all of your financial institutions and advise them that your cards have either been stolen or lost. If you just tell them that you *believe* that you are a victim of identity theft they will not cancel your credit card, they will simply put an alert on your account. In some cases an alert is not enough to stop recent transactions that are not yet posted onto your account. Make sure you report them stolen or lost so that they can immediately put a hold on any transactions on your account and have them issue new credit cards with new numbers. Some institutions may require written documentation to begin investigating your claim, so make sure you have all the information readily available.

You should also contact both of Canada's national credit reporting agencies, Trans Union Canada and Equifax Canada. Ask them to place a fraud alert, stating that creditors are to contact you prior to opening any new accounts or changing your existing accounts. Ask them to also send you a copy of your credit report so that you can see which accounts have been affected by this identity theft.

The next thing to do is report the matter to the police. They will require you make a written statement and will include your statement on their police report. You will receive a case number. Your creditor needs this case number in order to view a copy of the police report which states that this is a legitimate case. They can begin to correct any balances or refund any money to your accounts.

You should then call and report the incident to PhoneBusters National Call Centre. PhoneBusters is the Canadian Anti-fraud Call Centre. They gather information and intelligence about identity theft, and will provide you with advice and assistance.

Any Government issued documents that may have been lost or stolen should be reported to the responsible ministry or department and new documents should be requested.

Conclusion

The threat of identity theft is something we must all be aware of and be vigilant against. Understanding the value of pieces of personal identification, who we should and shouldn't share this identification with, and how to protect it are all crucial in fighting against this crime. The techniques that criminals use to gather our personal information can be quite "low-tech". Dumpster diving and mail redirection are examples of these unsophisticated schemes. Other techniques, however, are quite sophisticated, for example, phishing and card skimming. Although our government and the agencies responsible for issuing forms of identification or are aware of the problem of identity theft and are slowly addressing the issue, it is still in our best interest to take steps to prevent these crimes from happening to us. Unfortunately, many of us have already become a victim of identity theft. When that happens, there are several things you can do to stop the theft from continuing, and to begin the process of repairing the damage that has been done.

There is no quick fix to this problem. Being aware of the value of our personal information, of how identity thieves operate, of how we can protect ourselves, and knowing what to do if it happens to us, can help us in the fight against identity theft.

Resources for Canadian Victims of Identity Theft

PhoneBusters National Call Centre (PNCC)
Ontario Provincial Police Anti-Rackets
Toll Free: (888) 495-8501
Toll Free Fax: (888) 654-9426
Email: info@phonebusters.com
Web: www.phonebusters.com

Credit Reporting Agencies

Equifax Canada
Toll Free: (800) 465-7166
Web: www.equifax.ca

Trans Union Canada
Toll Free: (877) IDTHEFT (438-4338)
Web: www.tuc.ca

Resources for American Victims of Identity Theft

Equifax
Toll Free: (800) 525-6285
Web: www.Equifax.com

Experian
Toll Free: (888) EXPERIAN (397-3742)
Web: www.experian.com

Trans Union
Toll Free: (800) 916-8800
Web: www.transunion.com

For more information please visit:
(http://www.psepc-sppcc.gc.ca/publications/policing/Identity_Theft_Consumers_e.asp

Resources

Arnott, Sarah. “IT ends paper births register.” vnunet.com. 18 August 2004. URL:http://www.vnunet.com/print/1157422 (August 2004).

Bahadur, Cindy. “Identity Theft.” CBC Marketplace. 8 February 2000. URL:http://www.cbc.ca/consumers/market/files/scams/idtheft/ http://www.cbc.ca/consumers/market/files/scams/idtheft/index2.html (August 2004).

Banerjee, Scott. “What's your online broker doing to prevent ID theft?” CBS MarketWatch. 21 November 2003. URL:http://www.globalsecurity.org/org/news/2003/031121-id-theft01.htm (August 2004).

Bergstein, Brian. “Freeze hinders identity theft, but credit bureaus dislike it.” FortWayne.com. 9 August 2004. URL:http://www.fortwayne.com/mld/journalgazette/business/9355161.html (August 2004).

Bruce, Laura. “Is identity theft protection worth the money?” Bankrate.com. 4 August 2004. URL:http://www.bankrate.com/brm/news/advice/scams/20040804a1.asp (August 2004).

Canada Post. “Other Products and Services - Mail Redirection (Permanent).” August 2004. URL:http://www.canadapost.ca/common/offerings/supplementary_services_pers/can/redirection_permanent-e.asp (August 2004).

Canada Post. “Other Products and Services – Hold Mail.” August 2004. URL:http://www.canadapost.ca/common/offerings/supplementary_services_pers/can/hold-e.asp (August 2004).

Canadian Bankers Association. “Fraud and Security – Identity Theft.” cba.ca. August 2004. URL:http://www.cba.ca/en/section.asp?fl=4&sl=268&tl=276&docid (August 2004).

“Canadians Overwhelmingly Concerned about Identity Theft, but Most Do Not Know How to Protect Themselves, Finds New Intersections Inc./Ipsos-Reid Poll.” Yahoo!Finance. 30 June 2004. URL:http://biz.yahoo.com/bw/040630/305235_1.html (July 2004).

Carlson, Caron. “Congress Passes ID Theft Bill.” eweek.com. 25 June 2004. URL:http://www.eweek.com/print_article/0,1761,a=130306,00.asp (August 2004).

Chua, June. “Identity Theft - How Is It Done?” CBC News. 7 November 2003. URL:http://www.cbc.ca/consumers/indepth/identity/index2.html (August 2004).

Chua, June. “Identity Theft - Robbery in the New Millennium.” CBC News. 7 November 2003. URL:http://www.cbc.ca/consumers/indepth/identity/index.html (August 2004).

Department of Canada, Government of Newfoundland and Labrador. “Tips for Reducing the Risk of Identity Theft.” 18 August 2004. URL:http://www.gov.nf.ca/gs/cca/tpl/ident.stm (August 2004).

Foley, Linda. “Fact Sheet 117: Identity Theft and the Deceased: Prevention and Victim Tips.” Identity Theft Resource Center. January 2003. URL:http://www.idtheftcenter.org/vg117.shtml (August 2004).

Foley, Linda. “Fact Sheet 121: Identity Theft Prevention for Job Seekers.” Identity Theft Resource Center. July 2003. URL:http://www.idtheftcenter.org/vg121.shtml (August 2004).

Gaur, Nalneesh. “Hooked.” Information Security. July 2004. URL:http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss426_art874,00.html?track=NL-358&ad=487004 (August 2004).

Government of Canada. “Social Insurance Number (SIN) – Frequently asked Questions.” 19 August 2004. URL:http://www.sdc.gc.ca/asp/gateway.asp?hr=/en/cs/sin/030.shtml&hs=sxn#q20 (September 2004).

Government of Canada. “Social Insurance Number (SIN) – Proof-of-Identity Requirements.” 19 August 2004. URL:http://www.sdc.gc.ca/asp/gateway.asp?hr=/en/cs/sin/100.shtml&hs=sxn (August 2004).

Greek, Dinah. “Police warn on key-logging spam Trojan.” vnunet.com. 13 August 2004. URL:http://www.vnunet.com/print/1157314 (August 2004).

Hartsock, Nettie. “Anti-Phishing Working Group releases phishing report for June 2004.” WebDeviq.com. 8 August 2004. URL:http://www.webdeviq.com/news/1486-WebDevIQ_News.html (August 2004).

Hulme, George V. “President Signs Identity-Theft Law.” InformationWeek.com. 16 July 2004. URL:http://informationweek.com/story/showArticle.jhtml?articleID=23901861 (August 2004).

Human Resources Development Canada, Government of Canada. “Changes to protect the integrity of the Social Insurance Number.” 8 October 2002. URL:http://www.hrsdc.gc.ca/en/cs/comm/news/2002/021008_e.shtml (August 2004).

Information Service, Parliament of Canada. “Taking the necessary measures to enhance the integrity of the Social Insurance Number: A review of the Action Plan.” 25 February 2003. URL:http://www.parl.gc.ca/InfoComDoc/37/2/HUMA/Studies/Reports/humarp02/06-rap-e.htm (August 2004).

James, Peter. “Canadian credit monitoring is your best chance preventing identity theft in Canada.” CanadianCreditCenter.com. August 2004. URL:http://www.canadiancreditcenter.com/Canada-Credit-Monitoring.htm (August 2004).

KATU 2 News. “Cyber thieves are ‘Phishing’ for your money.” katu.com. 11 August 2004. URL:http://www.katu.com/printstory.asp?ID=70019 (August 2004).

King, Jason. “National Poll Indicates Americans Favor Congressional Action to Strengthen Driver’s License/ID Security.” aamva.org. 15 April 2002. URL:http://www.aamva.org/news/nwsPressReleaseNationalPollIndicatesAmericansFavorStrongerID.asp (August 2004)

Leyden, John. “UK Police issue ‘vicious’ Trojan Alert.” The Register. 13 August 2004. URL:http://www.theregister.co.uk/2004/08/13/trojan_phish/ (August 2004).

Lorenz, Kate. “Is the boss spying on you? - Follow 12 tips to help keep you privacy at work.” CareerBuilder.com. 13 August 2004. URL:http://edition.cnn.com/2004/US/Careers/08/13/boss.spying (August 2004).

McGuire, David. “House OKs More Jail Time for ID Thieves.” WashingtonPost.com. 23 June 2004. URL:http://www.washingtonpost.com/ac2/wp-dyn/A190-2004Jun23 (July 2004).

McGuire, David. “Fed, Private Groups to Educate Consumers About Phishing Scams.” SecurityFocus.com. 17 June 2004. URL:http://www.securityfocus.com/news/8936 (August 2004).

Mills, Kelly. “Bank questions ID fraud survey.” news.com.au. 5 August 2004. URL:http://www.News.com.au/common/printpage/0,6093,10345638,00.html (August 2004).

Ministry of Consumer and Business Services, Government of Ontario. “Identity Theft - Companies that Accept the Identity Theft Statement.” 2002. URL:http://www.cbs.gov.on.ca/mcbs/english/IDstatement_endorsers.htm (August 2004).

Ministry of Consumer and Business Services, Government of Ontario. “Identity Theft - The Identity Theft Statement: Frequently Asked Questions.” 2002 URL:http://www.cbs.gov.on.ca/mcbs/english/IDstatement_faq.htm (August 2004).

Ministry of Health Services, Government of British Columbia – Vital Statistics Agency. “British Columbia Birth Event.” August 2004. URL:http://www.vs.gov.bc.ca/births/index.html (August 2004).

Office of the Privacy Commissioner of Canada, Government of Canada. “Social Insurance Numbers (SIN).” 9 July 2004. URL:http://www.privcom.gc.ca/fs-fi/02_05_d_02_e.asp (August 2004).

Office of the Privacy Commissioner of Canada. “Identity Theft: What it is and what you can do about it.” 24 August 2004. URL:http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp (August 2004).

Passport Office, Government of Canada. “Frequently asked Questions.” 8 August 2004. URL:http://www.ppt.gc.ca/faq/index_e.asp#231 (August 2004).

Phone Busters, The Canadian Anti-Fraud Call Centre. “Identity Theft: Could it happen to you?” August 2004. URL:http://www.phonebusters.com/english/recognizeit_identitythe.html (August 2004).

Phone Busters, The Canadian Anti-Fraud Call Centre. “Identity Theft: Tips that will help minimize your risk.” August 2004. URL:http://www.phonebusters.com/english/recognizeit_identitythetips.html (August 2004).

Public Safety and Emergency Preparedness Canada, Government of Canada. “Public Advisory: Special Report for Consumers on IDENTITY THEFT.” 21 May 2003. URL:http://www.psepc-sppcc.gc.ca/publications/policing/Identity_Theft_Consumers_e.asp (August 2004)

Rees, Chris. “Consumer Alert: Cell phone camera identity theft.” WISTv.com. 2 August 2004. URL:http://www.wistv.com/global/story.asp?s=2119599&ClientType=Printable (August 2004).

Royal Canadian Mounted Police, Government of Canada. “Identity Theft.” 22 December 2003.
URL:http://www.rcmp-grc.gc.ca/scams/identity_e.htm (August 2004).

Smith, Portsia. “New law to help curb rise in identity theft.” fredricksburg.com. 12 August 2004.
URL:http://www.fredericksburg.com/News/FLS/2004/082004/08122004/1461570 (August 2004).

Social Security Administration. “Identity Theft and Your Social Security Number.” SSA Publication No. 05-10064, February 2004, ICN 463270
URL:http://www.ssa.gov/pubs/10064.html (August 2004).

Staff, Drivers.com. “Getting a driver's license.” Drivers.com 12 June 2000.
URL:http://www.drivers.com/article/294/ (August 2004).

Staff, Expositor. “Identity Theft in Canada: Fastest growing business is Canadian identity theft protection.” CanadianCreditCenter.com. 1 February 2003.
URL:http://www.canadiancreditcenter.com/articles/CCC-CANADIAN-IDENTITY-THEFT.htm (August 2004).

Sullivan, Bob. “Consumers still falling for phish - Fake e-mails fool users 28 percent of the time, study finds.” MSNBC.com. 28 July 2004.
URL:http://www.msnbc.msn.com/id/5519990/print/1/dispalymode/1098/ (August 2004).

Sullivan, Bob. “Kerry donors targeted by fake e-mail - Would-be contributors instead gave info to hacker.” MSNBC.com. 2 August 2004.
URL:http://www.msnbc.msn.com/id/5581739/print/1/displaymode/1098/ (August 2004).

Sullivan, Bob “Survey: 2 million bank accounts robbed - Criminals taking advantage of online banking, Gartner says.” MSNBC.com. 14 June 2004.
URL:http://www.msnbc.msn.com/id/5184077/print/1/displaymode/1098/ (August 2004).

TechWeb News, InformationWeek. “Sender Authentication Seen as Key to End Phishing.” InformationWeek.com. 28 June 2004.
URL:http://www.informationweek.com/showArticle.jhtml?articleID=22102466 (July 2004).

The Revised Statutes and Consolidated Regulations of British Columbia. “Motor Vehicle Act - Continued [RSBC 1996] CHAPTER 318.” August 2004.
URL:http://www.qp.gov.bc.ca/statreg/stat/M/96318_01.htm#section71 (August 2004).

Thomas, Daniel. “Online fraudsters target UK users.” vnunet.com. 19 August 2004.
URL:http://www.vnunet.com/print/1157442 (August 2004).

University of Nebraska Lincoln. Access-egov. “Glossary.” August 2001.
URL:http://www.access-egov.info/glossary.cfm?xid=NE (August 2004).

Ward, Susan. “The 5 Most Common Business Scams and How to Avoid them.” sbinfocanada.about.com. August 2004.
URL:http://www.sbinfocanada.about.com/od/scams/a/commonscams.htm (August 2004).

Watson, James. “Impact of Phishing now equals virus outbreaks.” computing.co.uk. 11 August 2004.
URL:http://vnunet.com/print/1157239 (August 2004).

Weston, Liz Pulliam. “The newest identity thieves: parents.” moneycentral.msn.com. August 2004.
URL:http://www.moneycentral.msn.com/content/Banking/FinancialPrivacy/P77623.asp?Printer (August 2004).

Wuorio, Jeff. “Protect your privacy: 10 simple steps.” moneycentral.msn.com. August 2004.
URL:http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P33715.asp (August 2004).

Unknown Author. “New Residents – Getting a License.” Cometobc.com. August 2004.
URL:http://www.cometobc.com/getdl.html (August 2004).